The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
05/18/2016

SUBJECT:
Multiple Vulnerabilities in VMware Products Could Allow Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in VMware products including vCenter, vCloud, vSphere, vROps, Workstation, and Player. Successful exploitation could potentially allow an attacker to cause deserialization flaws, execute commands, or elevate privileges.

SYSTEMS AFFECTED:
- vCenter Server
- vCloud Director
- vSphere Replication
- vROps non-appliance

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities**: Low**

Home users: Low

TECHNICAL SUMMARY:
VMware products are prone to multiple vulnerabilities that could allow for unauthorized access. These vulnerabilities are as follows:
- The RMI server of Oracle JRE JMX deserializes any class when deserializing authentication credentials. This may allow a remote, unauthenticated attacker to cause deserialization flaws and execute their commands.
- VMware Workstation and Player for Windows do not properly reference one of their executables. This may allow a local attacker on the host to elevate their privileges.

RECOMMENDATIONS:
The following actions should be taken:
- Install the updates provided by VMware immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on the system before applying patches.
- Monitor intrusion detection systems for any signs of anomalous activity.

REFERENCES:
VMware:
https://www.vmware.com/security/advisories/VMSA-2016-0005.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2077
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3427

SANS:
https://isc.sans.edu/diary/VMWare+Security+Advisories+VMSA-2016-0005/21071